IN THE UNITED STATES PATENT & TRADEMARK OFFICE

ART UNIT: 2155 EXAMINER: Thu Ha Nguyen APPLICANT: Sanchaita Datta and Ragula Bhaskar SERIAL NO.: 10/034,197 FILED: December 28, 2001 FOR: COMBINING CONNECTIONS FOR PARALLEL ACCESS TO MULTIPLE FRAME RELAY AND OTHER PRIVATE NETWORKS	**THRICE REVISED SUBSTITUTE APPEAL BRIEF** **CERTIFICATE OF TRANSMISSION** I certify that this paper is being submitted through EFS-WEB to the Commissioner for Patents on January 17, 2007. Printed Name: John W. Ogilvie

Commissioner for Patents:

This case was **made special** by a Decision mailed October 8, 2003.

On August 17, 2004, Appellants filed an Original Brief appealing from a Final Action mailed April 19, 2004. On December 23, 2004, the Examiner reopened prosecution by mailing a Reopening Action. On March 4, 2005, Appellants filed a Supplemental Brief. An Examiner's Answer was mailed three months later, on June 17, 2005, and Appellants' Reply was filed ten days after that, on June 27, 2005. Several months later, on November 10, 2005, the Board remanded the case to the Examiner. Appellants filed a Substitute Appeal Brief eleven days later, on November 21, 2005. Almost six months after that, on June 14, 2006, the Office mailed a Notification of Non-Compliant Brief. A Revised

Substitute Brief was filed five days later, in response to the Notification. Appellants submit that the Substitute Brief was adequate for appeal, but to avoid further delay added material shown in the Revised Substitute Brief in underlined italics. A second Notification of Non-Compliant Brief was mailed September 8, 2006, and a Twice Revised Substitute Brief was filed in response.

After a third Notification of Non-Compliant Brief was mailed January 11, 2007, the undersigned contacted the Examiner's supervisor, SPE Saleh Najjar, on January 16, 2007 by leaving a voicemail request for clarification. SPE Najjar responded the following day, identifying during a phone conference three claim limitations for which no reference numbers had been included in the recitation of independent claims in the Summary of Claimed Subject Matter. The Office's request for "another supplemental 'Artifact of 10/034/197ZA'" made in the Notification was also clarified by SPE Najjar. The undersigned thanks SPE Najjar for making clear the reasons for objecting to the appeal briefs. The objections have been addressed by changes below.

Real Party in Interest

The real party in interest in this appeal is Assignee, Ragula Systems (FatPipe Networks).

Related Appeals and Interferences

None.

Status of Claims

Claims 1-21 were rejected in the Final Action, were rejected in the

Reopening Action (December 23, 2004), are still pending, and are appealed.

Status of Amendments

No amendments were filed after the Final Action or the Reopening Action.

Summary of Claimed Subject Matter

The present invention relates to tools and techniques for accessing multiple independent frame relay networks and/or point-to-point (e.g., T1 or T3) network connections in a parallel network configuration, as shown for instance in Figure 5 or Figure 6. Frame relay networks 106 and point-to-point networks are each "private networks"; *see* application at page 9 lines 10-12. In some embodiments a controller 502 according to the invention comprises a site interface 702 connecting the controller to a site 102, at least two private network interfaces 706, and a packet path selector 704 which selects between private network interfaces according to a specified criterion. A site may include a local area network; *see* discussion of Figure 7 on pages 13-14, and page 17 lines 15-17.

The controller receives 804 a packet through the site interface and sends 814 the packet through the private network interface that was selected 806 by the packet path selector. The controller's packet path selector selects between private network interfaces according to various criteria, such as (a) a load-balancing criterion 808 that promotes balanced loads on devices that carry packets after the packets leave the selected private network interfaces; (b) a reliability criterion 810 that promotes use of devices that will still carry packets after the packets leave the selected private network interfaces, when other devices that could have been selected are not functioning, and (c) a security criterion 812 that promotes use of multiple private

networks to carry different pieces of a given message so that unauthorized interception of packets on fewer than all of the networks used to carry the message will not provide the total content of the message.

In response to point 4 of the first Notification, figure reference numbers are used in corresponding text in this application, as is the case in many patent applications, and correlating the above information with the independent claims readily yields the following:

1. A controller (502) which controls access to multiple independent private networks (application at page 9 lines 10-12) in a parallel network configuration, the controller comprising:

a site interface (702) connecting the controller to a site (102);

at least two private network interfaces (706); and

a packet path selector (704) which selects between private network interfaces according to a specified criterion;

wherein the controller receives (804) a packet through the site interface and sends (814) the packet through the private network interface that was selected (806) by the packet path selector.

13. A method for combining connections for access to multiple parallel private networks (application at page 9 lines 10-12), the method comprising the steps of:

obtaining a controller (502), the controller comprising a site interface (702), at least two private network interfaces (706), and a packet path selector (704) which selects between private network interfaces according to a specified criterion;

connecting the controller site interface to a site (102) to receive (804) packets from a computer at the site;

connecting a first private network interface (706) of the controller to a first private network;

connecting a second private network interface (706) of the controller to a second private network which is parallel to and independent of the first private network; and

sending (814) a packet to the site interface which then sends the packet through a private network interface selected (806) by the packet path selector.

19. A method for combining connections for access to multiple independent parallel frame relay networks, the method comprising the steps of:

sending (814) a packet to a site interface of a controller (502), the controller comprising the site interface (702) which receives (804) packets, at least two network interfaces (706), and a packet path selector (704) which selects between network interfaces according to a specified criterion; and

specifying the criterion for use by the packet path selector (704), wherein the specified criterion is one of: a security criterion, a reliability criterion, a load-balancing criterion.

The invention also provides other controller embodiments, and it provides method embodiments. The claims define the invention; this summary is provided merely as an introduction and to assist in understanding the claims.

Grounds of Rejection to be Reviewed on Appeal

1. Is a local area network a "private network" as that term is defined by applicants?
2. Were claims 9, 15 properly rejected under Section 103 in view of U.S. Patent No. 5,948,069 by Kitai et al. ("Kitai")?
3. Were claims 1-3, 8, 10-12, 14, 18, and 20 properly rejected under Section 103 in view of Kitai combined with U.S. Patent No. 6,209,039 to Albright et al. ("Albright")?
4. Were claims 4, 13, 16, and 21 properly rejected under Section 103 in view of Kitai combined with Albright and with U.S. Patent No. 5,910,951 to Pearce et al. ("Pearce")?
5. Was claim 5 properly rejected under Section 103 in view of Kitai combined with Albright and with U.S. Patent No. 6,546,423 to Dutta et al. ("Dutta")?
6. Was claim 17 properly rejected under Section 103 in view of Kitai combined with Albright, Pearce, and Dutta?
7. Were claims 6 and 7 properly rejected under Section 103 in view of Kitai combined with Albright and with U.S. Patent No. 6,195,680 to Goldszmidt et al. ("Goldszmidt")?
8. Was claim 19 properly rejected under Section 103 in view of Kitai combined with Pearce and also combined with Goldszmidt?

Note: The foregoing statement of issues resolves inconsistencies in the Reopening Action by following the actual reference citations that were made claim-by-claim in the Reopening Action, rather than following the summary paragraphs therein. For instance, summary paragraph 4 of the Reopening

Action asserts that several claims, including claim 9, are rejected in view of Kitai and Albright, but the actual rejection in paragraph 9 of the Reopening Action only cites Kitai. Therefore, claim 9 is treated here as being rejected in view of Kitai alone. Several similar inconsistencies in the Reopening Action are likewise resolved by addressing the references that were actually discussed in a rejection, rather than the references that a summary paragraph merely asserted (wrongly) would be discussed.

Argument

By way of context, the following papers are among those filed or mailed in this case:

Provisional	provisional application, filed December 29, 2000
Application	non-provisional application, filed December 28, 2001
First IDS	information disclosure statement, filed April 29, 2002
Second IDS	information disclosure statement, filed March 14, 2003
Third IDS	information disclosure statement, filed April 9, 2003
Fourth IDS	information disclosure statement, filed April 11, 2003
Petition	petition to accelerate examination, filed April 21, 2003
Fifth IDS	information disclosure statement, filed June 3, 2003
Petition Grant	decision granting Petition, mailed October 8, 2003
First Action	first office action on the merits, mailed November 5, 2003
Response	response, filed February 4, 2004
Third-Party	third party submission, filed on or about April 5, 2004
Final Action	final office action, mailed April 19, 2004
Interview Summary	interview summary, filed May 25, 2004

Appeal Notice	notice of appeal, filed July 14, 2004
Advisory Action	advisory office action, mailed July 23, 2004
Original Brief	appeal brief, filed August 17, 2004
Reopening Action	office action, mailed December 23, 2004
Supplemental Brief	appeal brief, filed March 4, 2005
Examiner's Answer	answer, mailed June 16, 2005
Supplemental Reply	reply, filed June 27, 2005
Remand Order	Board order, mailed October 10, 2005
Substitute Brief	appeal brief, filed November 21, 2005
Second Substitute Brief	filed September 12, 2006
Third Substitute Brief	present brief

The shortcomings of the rejections are reviewed below. Arguments and statements by Applicants made earlier but not repeated here are also part of the record for this appeal and are not waived, although they may be modified or supplemented here. To keep this brief short while still trying to provide an adequate basis for review, some observations and arguments that might have been presented are not included. Accordingly, Applicants' silence here with respect to particular statements by the Office does not indicate their agreement or acquiescence.

Third Party Submission

The Final Action does not refer to the third-party submission that was filed, on behalf of an unidentified third party, on or about April 5, 2004. References were submitted to the Office by a third party in each of the following applications of the

Assignee: 10/034190, 10/034197, 10/361837, 10/263497. That submission was made two weeks before the mailing of the Final Action, but it was not clear to the undersigned whether the Examiner had received and considered the submission's references. In response to the Examiner's Request in the Notification mailed June 14, 2006, a copy of the third party submission's non-patent references was submitted with the Revised Substitute Brief. In response to SPE Najjar's request, a higher-contrast (more easily read) copy of the third party submission is given here, in the Evidence Appendix.

Grouping of Claims

The grouping of claims for the appeal has been unsettled.

The Examiner's Answer states one grouping of claims on page 2, asserts on that page that this claim grouping was recited in Appellants' brief, and then repeats the grounds for rejection that were stated in the Reopening Action. However, the grouping of claims stated on page 2 of the Examiner's Answer was *not* recited in Appellants' brief, and it does *not* follow the structure of the rejections stated in the Reopening Action.

Page 2 of the Examiner's Answer identifies three claim groups:

Claims 1, 2-12;
Claims 13, 14-18; and
Claims 19, 20-21.

But these three groups are not consistent with Appellants' Brief or with the stated grounds for rejection. This claim grouping (three groups: 1-12, 13-18, 19-21) given in the Answer is not accepted by Appellants.

Page 4 of the Supplemental Brief identified seven claim groups:

Group I: claims 9, 15
Group II: claims 1-3, 8, 10-12, 14, 18, and 20
Group III: claims 4, 13, 16, and 21
Group IV: claim 5
Group V: claim 17
Group VI: claims 6 and 7
Group VII: claim 19

This grouping generally tracks the Reopening Action grounds, by grouping claims that are rejected on the same grounds and for which there is also clearly a discussion of all cited references. This approach is explained in the Supplemental Brief on pages 3 and 4, in the presentation of issues and claim groupings. However, this approach could be seen as departing from the rejections' structure by separating claims 9 and 15 into their own group.

Arrival at an appropriate claim grouping is further complicated by the fact that the Examiner's Answer is not internally consistent. On page 2, the Answer identifies three claim groupings, but on pages 3-17 it repeats rejections (made in the Reopening Action) that use more than three groupings.

In short, without further action, the Board will face multiple inconsistent claim groupings. This could hamper a full, efficient, and fair review of the claims. In the interest of promoting such review, and in a spirit of compromise with the Examiner, Appellants hereby agree to modify the claim grouping of their Supplemental Brief by treating claim 9 as standing or falling with its parent claim 1, and by treating claim 15 as standing or falling with its parent claim 13. The resulting claim grouping follows the structure of the rejections and reduces the number of claim groups by one.

Pursuant to M.P.E.P. § 1206, Appellants therefore submit the six (not seven) claim groups shown below. Please refer to the Reopening Action and the appeal Briefs for identification and discussion of the specific claim limitations involved. Within each of these six groups, the claims stand or fall together.

(Group) claims	References cited	Sample reasons for patentability
(II) claims 1-3, 8, 9, 10-12, 14, 18, and 20	Kitai + Albright	Kitai + Albright combination is not supported; see Supp. Appeal Brief at 6-7, Orig. Appeal Brief at 13-14: no motive to combine frame relay reference Albright w/ LAN reference Kitai; no motive to combine serial reference Albright w/ parallel reference Kitai
(III) claims 4, 13, 15, 16, and 21	Kitai + Albright + Pearce	Kitai + Albright combination is not supported per Group II arguments; no evidence showing motive to add Pearce, see Orig. Appeal Brief at 10-11
(IV) claim 5	Kitai + Albright + Dutta	Kitai + Albright combination is not supported per Group II arguments; no evidence showing motive to add Dutta, see Orig. Appeal Brief at 11-12
(V) claim 17	Kitai + Albright + Pearce + Dutta	Kitai + Albright combination is not supported per Group II arguments; no evidence showing motive to add Pearce, see Orig. Appeal Brief at 10-11; no evidence showing motive to add Dutta, see Orig. Appeal Brief at 11-12
(VI) claims 6 and 7	Kitai + Albright + Goldszmidt	Kitai + Albright combination is not supported per Group II arguments; no evidence showing motive to add Goldszmidt, see Orig. Appeal Brief at 12-13
(VII) claim 19	Kitai + Pearce + Goldszmidt	Kitai + Pearce combination is not supported, see Orig. Appeal Brief at 10-11; Kitai + Goldszmidt combination is not supported, see Orig. Appeal Brief at 12-13

Reply to Examiner's Responses

On pages 17-24, the Examiner's Answer responds to arguments made by Appellants. It may be helpful to begin with these arguments, and work backward from there as needed. In reply to the Answer, Appellants respectfully submit that the claims are patentable and the rejections are flawed.

Examiner's response (A) seeks to reverse the Examiner's position by arguing that local area networks as disclosed in Kitai are actually "private networks" as claimed. The only basis given for this reversal in the Answer is that "the examiner reopened the Office action with new ground of rejection." This is not a sufficient basis to support the change in position. Indeed, the Reopening Action admits in its discussion of claim 1 that "Kitai does not explicitly teach at least two private network interfaces" and it then relies on Albright to teach private network interfaces. As explained at length in both the Original Brief at pages 5-9 and the Supplemental Brief at pages 5-6, Kitai does not teach private networks. This lack of teaching in Kitai is pertinent, not only because it makes Kitai unusable as a Section 102 reference, but also under Section 103 because it draws one of skill away from the asserted Kitai-Albright combination, as explained in the appeal Briefs.

Examiner's response (B) argues that Kitai taken alone under Section 103 is grounds for rejecting claims 9 and 15, because private networks are not mentioned in those claims. But this argument fails to recognize that claims 9 and 15 include the limitations of their respective parent claims, which do expressly require private networks.

Examiner's response (C) misunderstands Appellants' argument. The Examiner treats the argument as one that states the combination fails to teach the claimed invention because Albright teaches serial networks rather than parallel networks. The response therefore understandably notes that the failure of one reference in a combination to teach a contested feature does not show that the combination as a whole fails to teach the feature, and thus to teach the invention. That is, the Examiner's answer is basically that it doesn't matter that Albright fails to teach parallel networks, because Kitai does teach parallel networks.

But this answer is directed at the wrong argument. Appellants are not arguing that Kitai combined with Albright fails to teach parallel networks. Rather, Appellants argue that Kitai and Albright were not properly combined.

Appellants' claims were improperly used as a blueprint. In the Office Action mailed 11/05/2003, the Examiner made rejections using Kitai as a Section 102 reference. In the next Response, Appellants pointed out that Kitai does not teach private networks, and hence cannot support rejections under Section 102. In the final action mailed 04/19/2004, the Examiner asserted again that Kitai was a Section 102 reference. The Original Appeal Brief followed, in which pages 5 through 9 explained in detail and with supporting evidence why Kitai does not teach parallel networks and thus could not – by itself – support rejections. Instead of letting the appeal go to the Board, the Examiner then reopened prosecution. In the Reopening Action, the Examiner did *not* assert Kitai as a Section 102 reference. Instead, the Examiner made Section 103 rejections, supplementing Kitai by pointing to Albright for the necessary teaching of private networks. Of course, Albright cannot be used as a ground for rejection in combination with Kitai unless

there is some suggestion or motivation **in the art** for combining those references. There is not.

Appellants argue that Albright and Kitai were not properly combined, not merely because the Examiner failed to give any specific evidence of a motivation or suggestion in the art supporting that combination, but also because of the undisputed fact that Albright deals with *serial* networks – a fact which would have led those of skill in the art away from combining Albright with Kitai when they were trying to build a *parallel* network configuration.

In short, Appellants argue against making the Kitai + Albright combination in the first place, not against the teachings of that (improper) combination once it is made. This argument has not been rebutted. The Kitai + Albright combination is improper, regardless of what it teaches or fails to teach.

Examiner's response (D) cites a portion of Pearce as a suggestion or motivation for adding Pearce to the Kitai + Albright combination. But this fails to support the rejection.

As noted in the Appeal Briefs, the underlying Kitai + Albright combination is not proper.

Moreover, the cited portion of Pearce does not point toward the teachings of Kitai or Albright as possible solutions to some problem. Indeed, even if one interprets Pearce as treating the need for a prioritized list of qualifying networks as a problem, one sees that Pearce promptly provides its own solution in the form of a filter 38. The undersigned did not find in Pearce any suggestion that a reader should look elsewhere for serial network-to-network interfaces as described in Albright, or for a LAN switch as described in Kitai. Pearce is self-contained in this respect, and thus would not have instilled a motive to look elsewhere to enhance or

replace the filter 38. Accordingly, the combination of Pearce with Kitai and Albright is not proper.

Examiner's response (E) cites a portion of Dutta as a suggestion or motivation for adding Dutta to the Kitai + Albright combination. This fails to support the rejection.

As noted, the underlying Kitai + Albright combination is not proper.

Moreover, the cited portion of Dutta does not point toward the teachings of Kitai or Albright. As noted, e.g., on page 12 of the Original Brief, Dutta discusses firewalls and security while Kitai does not mention either. Albright discusses frame relay networks but Dutta does not. There is no evidence of any suggestion or motivation in Dutta that would have led one of skill to Kitai and Albright rather than somewhere else, and those of skill in the art did not have the claims to use as a blueprint. The combination of Dutta with Kitai and Albright is not proper.

Examiner's response (F) attempts to justify the even larger combination of Kitai, Albright, Pearce, and Dutta. As noted above and in the appeal Briefs (which are incorporated as part of the record before the Board), the sub-combination of Kitai with Albright is not proper, and neither are the combinations of three references obtained by adding Pearce or Dutta alone to Kitai and Albright. The only basis for combining these four references is impermissible hindsight, which is driven by Appellants' claims, not by the prior art.

Examiner's response (G) fails to rebut the argument made at pages 12-13 of the Original Brief. Goldszmidt does not teach *sending* packets out of sequence as claimed. Rather, Goldszmidt views such non-sequential packets as an unfortunate problem and concerns itself with ways to handle *receiving* packets out of sequence. Nor is there a motivation for combining the references – as noted, Kitai fails to

mention packet sequence, and the Kitai + Albright combination is not properly motivated.

Examiner's response (H) again tries to defend combining Kitai, Albright, and Dutta. As noted above, e.g., in regard to response (E), this combination is not proper.

Examiner's response (I) tries to defend combining Kitai, Pearce, and Goldszmidt. As noted above, e.g., in regard to responses (D) and (G), this combination is not proper.

We turn now to other arguments exchanged before this Substitute Appeal, and repeated here for convenience.

A local area network is not a "private network"

Despite the well-documented and detailed explanation of Kitai's shortcomings at pages 5-9 of the Original Appeal Brief (incorporated herein), the Examiner continues to assert Kitai in every rejection. The examiner now concedes (e.g., on pages 3, 5, 9 of the Reopening Action) that Kitai does not teach private networks; the LANs of Kitai are not private networks. The failure of Kitai to discuss private networks is one reason those of skill in the art would not have combined Kitai with other references, such as Albright, that do discuss frame relay or other private networks. Kitai's failure to discuss private networks is also a reason why the asserted combinations, even if they were proper, would fail to teach the claimed invention. However, these points are made at length in the Original Appeal Brief and below, so it suffices at this time to note that the Reopening Action (unlike the Final Action) does not argue that Kitai's local area networks are actually private networks as claimed by Applicants. Indeed, by withdrawing the rejections

under Section 102 which were based solely on Kitai, the Examiner has implicitly acknowledged that Kitai fails to teach private networks.

Claims 9 and 15 were not properly rejected under Section 103 in view of Kitai

The Reopening Action is inconsistent as to the basis for rejecting these claims. Although the preceding summary paragraphs in the Reopening Action (paragraphs 4 and 14) assert that these claims are rejected based on more references than just Kitai, the rejections themselves (paragraphs 9 and 18) only discuss Kitai. Accordingly, for purposes of appeal, the rejections are based solely on Kitai. However, if the Board wishes to consider other grounds *sua sponte*, with regard to these or other claims, then Applicants respectfully request that the Board please also consider the arguments here and in the Original Appeal Brief against combining Kitai with other cited references.

As noted, the Examiner concedes that Kitai fails to teach private networks. Moreover, the leap from Kitai's LANs to the claimed invention's private networks is a large and nonobvious leap, for at least the reasons discussed in the Original Appeal Brief at pages 6-9. Thus, the claims are not obvious in view of Kitai.

Claims 1-3, 8, 9, 10-12, 14, 18, and 20 (Group II) were not properly rejected under Section 103 in view of Kitai combined with Albright

The Original Appeal Brief noted on pages 13-14 the failure of the office actions up to that point to provide a proper justification for combining Kitai and Albright. The Reopening Action asserts different reasons, but they likewise fail to establish the necessary suggestion or motivation in the art for combining these references. On page 4 of the Reopening Action, the reason given is that the

combination "would provide an efficient communications system that the data can be dynamically monitored and routed among links/paths in order to reduce the congestion or failure within the networks (col. 2, lines 15-25)." But as in the Final Action, this rejection confuses serial networks with parallel networks. The cited section of Albright actually teaches routing *within* a network, not routing that selects between two parallel networks. Moreover, the rejection again fails to explain any reason why the cited section of Albright would have led one of skill in the art to Kitai, as opposed to any other reference.

Accordingly, the rejections based on Albright and Kitai should be withdrawn or reversed. The combination is improper because the cited section of Albright (a frame relay reference) does not suggest combination with Kitai (a LAN reference). Moreover, the combination fails to teach the claimed parallel private network innovations, because Albright teaches serial networks (they are in fact the very reason for Albright's network-to-network interface) rather than teaching networks placed in parallel as claimed.

Claims 4, 13, 15, 16, and 21 (Group III) were not properly rejected under Section 103 in view of Kitai combined with Albright and Pearce

The failure to justify combining Kitai and Albright is discussed above with respect to Group II claims, and in the Original Appeal Brief on pages 13-14. The Reopening Action fails to give any further basis for adding Pearce to this combination. For example, in paragraph 15, the Reopening Action merely asserts that it would have been obvious to combine Kitai, Albright and Pearce "because it would have an efficient communication system to control and select the reliable, qualifiable network/interface/path among multiple networks/interfaces/paths."

Paragraph 32 of the Reopening Action asserts that it would have been obvious to combine Kitai, Albright and Pearce "because it would detect and improve network security, traffic and failure." These are general statements, which do not suggest any combination of references. They merely suggest goals without suggesting ways to meet them.

The rejections fail to identify anything specific in one reference or in the art that would have led one of skill to the particular other references. It is well-established patent law that a rejection under Section 103 requires evidence of a suggestion or motivation in the prior art to combine the references. *See, e.g.,* M.P.E.P. §§ 2142, 2143.01, and cases cited therein. A general unsupported assertion that the combination would be efficient or more secure is not specific **evidence** that one of skill would have combined these particular references. For at least these reasons, the rejections should be withdrawn or reversed.

Claim 5 (Group IV) was not properly rejected under Section 103 in view of Kitai combined with Albright and Dutta

The failure to justify combining Kitai and Albright is discussed above with respect to Group II claims, and in the Original Appeal Brief on pages 13-14. The failure to justify combining Kitai and Dutta is discussed in the Original Appeal Brief on pages 11-12. The Reopening Action fails to add any grounds for combining these references. For at least these reasons, the rejections should be withdrawn or reversed.

Claim 17 (Group V) was not properly rejected under Section 103 in view of Kitai combined with Albright, Pearce, and Dutta

The failure to justify combining Kitai and Albright is discussed above with respect to Group II claims, and in the Original Appeal Brief on pages 13-14. The failure to justify combining Kitai and Dutta is discussed in the Original Appeal Brief on pages 11-12. The failure to justify combining Kitai and Pearce is discussed in the Original Appeal Brief on pages 10-11. The Reopening Action fails to add any grounds for combining these references. For at least these reasons, the rejections should be withdrawn or reversed.

Claims 6 and 7 (Group VI) were not properly rejected under Section 103 in view of Kitai combined with Albright and Goldszmidt

The failure to justify combining Kitai and Albright is discussed above with respect to Group II claims, and in the Original Appeal Brief on pages 13-14. The failure to justify combining Kitai and Goldszmidt is discussed in the Original Appeal Brief on pages 12-13. The Reopening Action fails to add any grounds for combining these references. For at least these reasons, the rejections should be withdrawn or reversed.

Claim 19 (Group VII) was not properly rejected under Section 103 in view of Kitai combined with Pearce and Goldszmidt

The failure to justify combining Kitai and Pearce is discussed in the Original Appeal Brief on pages 10-11. The failure to justify combining Kitai and Goldszmidt is discussed in the Original Appeal Brief on pages 12-13. The Reopening Action fails to add any grounds for combining these references. For at least these reasons, the rejections should be withdrawn or reversed.

Conclusion

For at least the reasons explained above, all rejections should be withdrawn or reversed. If any questions might be answered by telephone, the undersigned invites a call at the Office's convenience.

Please note that the **correspondence address below is different** than in earlier Briefs.

Dated this January 17, 2007.

Respectfully submitted,

JOHN W. OGILVIE
Registration No. 37,987

OGILVIE LAW FIRM
Customer No. 23484
1320 East Laird Avenue
Salt Lake City, Utah 84105
801-706-2546 (voice)
801-583-0393 (fax)

CLAIMS APPENDIX

1. A controller which controls access to multiple independent private networks in a parallel network configuration, the controller comprising:

a site interface connecting the controller to a site;

at least two private network interfaces; and

a packet path selector which selects between private network interfaces according to a specified criterion;

wherein the controller receives a packet through the site interface and sends the packet through the private network interface that was selected by the packet path selector.

2. The controller of claim 1, wherein the controller control access to multiple independent frame relay networks, and each of the at least two private network interfaces comprises a frame relay network interface.

3. The controller of claim 1, wherein the packet path selector selects between private network interfaces according to a load-balancing criterion, thereby promoting balanced loads on devices that carry packets after the packets leave the selected private network interfaces.

4. The controller of claim 1, wherein the packet path selector selects between private network interfaces according to a reliability criterion, thereby promoting use of devices that will still carry packets after the packets leave the

selected private network interfaces, when other devices that could have been selected are not functioning.

5. The controller of claim 1, wherein the packet path selector selects between private network interfaces according to a security criterion, thereby promoting use of multiple private networks to carry different pieces of a given message so that unauthorized interception of packets on fewer than all of the private networks used to carry the message will not provide the total content of the message.

6. The controller of claim 1, wherein the controller sends packets out of sequence over the parallel private networks.

7. The controller of claim 6, wherein the controller places an encrypted sequence number in at least some of the packets which are sent out of sequence.

8. The controller of claim 1, wherein the controller comprises at least three frame relay network interfaces, each of which is selectable by the packet path selector.

9. The controller of claim 1, wherein the controller operates in a system providing at least one point-to-point connection.

10. The controller of claim 1, wherein the controller operates in a system providing connectivity over at least two frame relay networks from at least two

carriers, each frame relay network operating on its own clock which is different from the clock of the other frame relay network.

11. The controller of claim 1, wherein each private network interface is an indirect interface tailored to a particular type of frame relay network.

12. The controller of claim 1, wherein each private network interface is a direct interface comprising an Ethernet card.

13. A method for combining connections for access to multiple parallel private networks, the method comprising the steps of:

obtaining a controller, the controller comprising a site interface, at least two private network interfaces, and a packet path selector which selects between private network interfaces according to a specified criterion;

connecting the controller site interface to a site to receive packets from a computer at the site;

connecting a first private network interface of the controller to a first private network;

connecting a second private network interface of the controller to a second private network which is parallel to and independent of the first private network; and

sending a packet to the site interface which then sends the packet through a private network interface selected by the packet path selector.

14. The method of claim 13, wherein the private networks are frame relay networks.

15. The method of claim 13, further comprising the step of specifying the criterion for use by the packet path selector, wherein the specified criterion is a load-balancing criterion.

16. The method of claim 13, further comprising the step of specifying the criterion for use by the packet path selector, wherein the specified criterion is a reliability criterion.

17. The method of claim 13, further comprising the step of specifying the criterion for use by the packet path selector, wherein the specified criterion is a security criterion.

18. The method of claim 13, wherein at least one of the steps connecting a private network interface of the controller connects the controller to a User-to-Network Interface in a router of a frame relay network.

19. A method for combining connections for access to multiple independent parallel frame relay networks, the method comprising the steps of:

sending a packet to a site interface of a controller, the controller comprising the site interface which receives packets, at least two network interfaces, and a packet path selector which selects between network interfaces according to a specified criterion; and

specifying the criterion for use by the packet path selector, wherein the specified criterion is one of: a security criterion, a reliability criterion, a load-balancing criterion.

20. The method of claim 19, wherein the step of sending a packet to the controller site interface is repeated as multiple packets are sent, the step of specifying a criterion specifies a security criterion, and the controller sends different packets of a given message to different frame relay networks.

21. The method of claim 19, further comprising the step of sensing failure of one of the parallel frame relay networks and automatically sending traffic through at least one other parallel frame relay network.

EVIDENCE APPENDIX

(contains non-patent literature from third party submission, requested by Examiner in Notification mailed 06/14/2006, and filed by Appellant on 06/19/2006; this copy is a re-scanned high-contrast copy per SPE Najjar's request)

Attorney Docket No.: 101092-00074

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor:	SANCHAITA DATTA
Confirmation No.:	7746
Serial No.:	10/034,197
Filed:	December 28, 2001
Title:	COMBINING CONNECTIONS FOR PARALLEL ACCESS...
Examiner:	THU HA T. NGUYEN
Group Art Unit:	2155

April 2, 2004

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

THIRD PARTY SUBMISSION

SIR:

Please withdraw the fees for this third party submission from deposit account 50-1290, as set forth in 37 CFR 1.17(p) and 37 CFR 1.17(i).

Submitted for consideration is the following documents and publication date:

1) U.S. Patent No. 6,665,702B1 Issued December 16, 2003;

2) "Radware announces LinkProof: The first IP Load Balancing Solution for networks with multiple ISP connection" Published October 7, 1999;

3) "Radware Balances the Network" Published January 7, 2000;

4) "Global Product Spotlight: Radware Linkproof" Published December 1, 1999;

5) "Radware Seeks Solutions to Easy-Access Problems" Published December 1, 1999;

This submission has been served upon the applicant in accordance with 37 CFR 1.248. Proof of service is attached.

This submission is after the two months from the time the application was published because:

1. The publication of the application only became known to the third party submitter on or about January 30, 2004; and
2. The U.S. patent issued on December 16, 2003, which was after the two month period had expired and therefore could not have been submitted within the time period.

Respectfully submitted,

_____

Brian S. Myers
Reg. No. 46,947

CUSTOMER NUMBER 026304
Telephone: (212) 940-8703
Fax: (212) 940-8986 or 8987
Docket No.: 101092-00074
BSM:fd

Radware announces LinkProof: The first IP Load Balancing Solution for networks with multiple ISP connection

Mahwah, NJ; October 7, 1999. To ensure 7x24 availability many enterprises, e-commerce sites and regional ISPs are utilizing multiple Internet router connections. The LinkProof by Radware (Nasdaq: RDWR) is the first technology designed to intelligently load balance IP traffic between these "multi-homed" sites, creating redundancy and eliminating single points of failure.

Deploying independent router connections to two or more ISPs creates these multi-homed sites. This diversity ensures 7x24 availability and an uninterrupted packet delivery to and from the enterprise in the event one or more ISP connection fails. While this adds redundancy, it also creates configuration complexity that may necessitate intricate routing protocols such as BGP (Border Gateway Protocol) and/or coordination between the contracted ISPs.

LinkProof removes this complexity by taking responsibility for the packet delivery through a healthy ISP connection. Sitting logically between the enterprise network and a farm of Internet routers, the LinkProof verifies ISP health and intelligently load balances all inbound and outbound traffic. In addition, it performs Smart NAT to ensure the uninterrupted packet delivery to and from the enterprise network. Smart NAT allows the LinkProof to perform network address translation according to the ISP connection selected to carry the session to the Internet. For example, if the LinkProof chooses ISP_1 for outbound session delivery, then the translated source address will belong to the ISP_1 IP address pool for the inbound response.

Internet traffic is optimized by the LinkProof through intelligent load balancing based on the current session and/or load per verified ISP connection. Additionally, network proximity is measured to determine the closest and fastest route. Network proximity is calculated in both router hops and round trip latency. This allows multi-homed sites to transmit information through a fast, healthy route.

LinkProof also uses proximity detection to perform inbound traffic management. For Internet users attempting to access a resource on the enterprise network (such as a Web server), the LinkProof uses DNS to assure the most optimal ISP connection. This feature allows the LinkProof to consistently use the best and quickest path to satisfy user requests for information.

The LinkProof continuously monitors the health of all routers in the farm, and periodically checks each router path and the health of user defined nodes beyond the router. This monitoring allows the LinkProof to continually send sessions through healthy routers on a healthy Internet path.

About Radware

Radware develops, manufacturers and markets products that manage and direct Internet traffic among network resources to enable continuous access to Web sites and other services, applications and content based on the Internet protocol. Radware offers a broad range of Internet traffic management solutions to service providers, e-commerce businesses and corporate enterprises that require uninterrupted availability and optimal

performance of IP-based applications that are critical to their business. Radware's Internet traffic management solutions enable its customers to manage their network infrastructure to bypass system failures and to scale their network infrastructure to accommodate increasing IP traffic. Radware's products improve the productivity of network infrastructure by distributing traffic within a network to optimize the use of available network resources. Radware's products can be deployed either as independent solutions to address specific application needs at a particular location within a network or as an end-to-end integrated solution to manage traffic throughout a network.

This press release contains forward-looking statements that are subject to risks and uncertainties. Factors that could cause actual results to differ materially from these forward-looking statements include, but are not limited to, general business conditions in the Internet traffic management industry, changes in demand for Internet traffic management products, the timing and amount or cancellation of orders and other risks detailed from time to time in Radware's filings with the Securities and Exchange Commission, including Radware's Form F-1.

Radware Balances the Network

Internet Traffic Management Center, January 1, 2000.

By Peter Christy

One of the absolutely thrilling parts of our job is being exposed to the continuing innovation of in the industry. We love watching the process of application invention - new ideas, seemingly out of the blue, that redefine "common knowledge" on what the product category is good for.

In the past, Alteon had some of our favorite inventions: cache redirection and balancing was certainly a good idea, and they invented a particularly cute DNS request capture application. This time we focus on Radware with LinkProof -- their invention for balancing and managing multi-homed connections out to the Internet.

Multi-homing is a simple concept. You want to have multiple connections to the Internet, provided by multiple ISPs. But multi-homing quickly gets very complicated, is difficult to configure, and is certainly not something you would want to reconfigure casually. Radware looked at this problem and developed an innovative application of traffic management.

For this discussion, let's assume a fairly simple multi-homing configuration: a branch office LAN connected to the Internet through two different ISPs. The obvious application of traffic management is simple life testing of the two links, and assuring that no traffic is sent to an ISP if a link is down. And you can imagine how a traffic manager could look at the load on the two links and balance it suitably.

But Radware goes well beyond this, using their DNS technology to determine which of the ISPs is the better path for specific traffic, and then routing traffic accordingly. This is clearly an innovative and clever use of traffic management, and certainly one we had never come close to imagining before. (See Radware's white paper for more interesting details.)

This kind of innovation is particularly important given a question we are regularly asked: "Won't the traffic management product category disappear over time as the functionality migrates into conventional routers and switches?" The answer we give is "Yes, if a traffic management company invents nothing new, then over time the value of that product will diminish." But we strongly feel that this is the wrong way to look at traffic management. In the server room, we see traffic management systems in effect becoming the operating system of the clustered computers that are serving out a return to centralized information systems. That's a big deal and a big future. And at the global level, we see the DNS solutions evolving into fairly full-blown content-directed routing schemes (as in the Akamai network), and that's also a very big deal. So the future of traffic management lies in innovation, and it's a significant and exciting future, if an unknown one.

Global Product Spotlight: Radware Linkproof

NetworkMagazine.com, December 1, 1999

Radware's new load balancer maximizes backup Internet links

By David Greenfield

What's an easy way to strengthen an Internet hookup? Add a link to another upstream Internet provider. That might be smart planning, but it doesn't make for great accounting. Backup links sit idle most of the time, which means ISPs pay full tariffs for rarely used lines.

Radware (www.radware.com) thinks there's a better business solution. Its new LinkProof is the first load balancer to make running parallel links to the Internet easy and cost-effective. For starters, LinkProof optimally distributes traffic across multiple access lines. What's more, if a line or router fails, LinkProof rolls the traffic over to the backup connections.

That might not sound like such a big deal. After all, tweaking the Border Gateway Protocol 4 (BGP4) routing protocol can yield similar benefits. But not everyone runs BGP4, and those who do spend considerable time and expense configuring the protocol. Finally, while BGP4 will switch to a backup link, the protocol won't let you weight your traffic distribution to maximize your connections. LinkProof will do all of that, and it doesn't require a Ph.D. to deploy.

Or so says Radware. Although there are plenty of users briefed on the product, nobody has tested it. What's more, none of these users are the second-tier ISPs that are supposed to adopt the product. Finally, because LinkProof only works with links on its subnet, the box can't distribute traffic loads across lines on other networks or offices.

Still, that's not stopping some major networkers from getting excited about the product. "On paper at least, LinkProof sounds like just what we want," says George Kurian, consultant of architecture and technology planning at Pacific Corp., a utility company in Portland, OR. Pacific currently runs its Internet access out of Portland, while paying for a backup link out of Salt Lake City, UT.

LinkProof, a modular box with two Ethernet or Fast Ethernet ports, sits between the firewall protecting the corporate backbone and in front of the routers connected to the Internet. At install-time, the network manager assigns a weight to each link that indicates the speed or cost of each line.

The rest of the configuration depends on the particular application. When load balancing incoming traffic, as is common with an e-commerce site, the LinkProof appears as the default DNS server. DNS queries from users looking to access the site are sent to LinkProof. It has IP addresses that are associated with each of the ISPs' links. LinkProof determines the optimum link based on latency and packet loss and then responds with the appropriate destination IP address.

When balancing outgoing Internet traffic, LinkProof is defined as the default router. It receives all outgoing packets and determines

the optimal link. LinkProof then changes the packet's source address to an address associated with an ISP's line and forwards the packet to the appropriate router.

So what happens in the event of a failure? LinkProof constantly monitors the health of each connection by testing the availability of up to 10 IP addresses along the path. If the address doesn't respond after some user-defined period of time, the traffic is directed to the alternative link. By default, the switch time is two seconds.

The key in both cases is Smart Network Address Translation (SmartNAT), which is the ability to reply with an IP address specific to a link. With SmartNAT, LinkProof insures that the client's responses return along the same link as the outgoing request. This enables LinkProof to account for traffic flowing in both directions when making a load-balancing decision. "Without SmartNAT, you don't get real load balancing," says Kurian.

Radware certainly isn't the only vendor in the load-balancing market. A number of other companies—including Alteon WebSystems, Foundry Networks, and F5 Networks —deliver products that distribute traffic across Web sites and firewalls.

However, they stumble when it comes to delivering SmartNAT capabilities. Alteon is close, but the implementation is too cumbersome, says Kurian. Foundry and F5 don't offer products with SmartNAT today. F5 says it will add the SmartNAT feature in the next release of BIG/ip, which is expected to ship in December 1999. Foundry has not announced plans for releasing SmartNAT.

Radware Seeks Solutions to Easy-Access Problems

South China Morning Post, December 7, 1999.

South China Morning Post
INTERNET EDITION

By Veronique Saunier

Continuous access to Web sites is at the core of every product developed by Radware, a small Israeli company that claims to be the second-largest vendor of Internet traffic-management solutions. "The Internet is cruel. For a company cashing on e-commerce, a down time of even one minute means lost business and lost customers who may never come back," said Yaron Danieli, Radware's vice-president of sales for Asia Pacific.

"Yet the Internet is vulnerable. Everything from traffic overload to a pulled Ethernet cable can make a Web server unavailable."

Maintaining Web sites to keep them up and running continuously has become a business in itself for many companies, including France Telecom Hebergement - the host of the prestigious Presidency of Republic of France site - or Sprint IP Web hosting.

These carriers guarantee 100 per cent availability and offer their customers financial compensation if their sites are down for even a few seconds.

The way they keep their promises without bankruptcy is by making every machine and circuit of the network redundant by ensuring if one machine breaks the other still operates.

They also place so-called "load balancers" at strategic points of the network to make the Internet as fluid and fast as possible.

Although the concept of load balancing is quite simple - it directs Internet traffic to the server that is ess busy - Radware claims it pioneered the concept and has been perfecting it since the launch of Web Server Director (WSD) four years ago.

WSD won Radware top honours from several United States technical magazines for its management, configuration, and ability to act as both primary and secondary load balancer at once.

Follow-up products include WSD Pro, which supports multiple networks, WSD DS which dispatches traffic to the nearest server in

the case of distributed sites, and Cache Server Director which intercepts Web users' requests and directs them to the most available cache server.

High availability also has become a critical component of firewalls deployed across enterprise networks to provide secure connectivity for Internet, and intranet and extranet communications.

Last year Radware launched FireProof, which load balances data to the best available firewall of the network.

According to Mr Danieli, many Cisco Systems' firewalls are load balanced by Radware's FireProof.

"While we were installing FireProof, we realised many companies wished to have multiple connections to the Internet instead of relying on one single ISP but were not ready to go through the hassles," Sharon Trachtman, vice-president marketing, said.

Using multiple ISPs adds redundancy abilities but necessitates complex configuration and routing protocols as well as close co-ordination between the contracted ISPs.

To make things easier, Radware designed a dedicated product that determined the closest, fastest and healthiest route for incoming and out-bound IP traffic between different ISPs.

That product, LinkProof, was launched globally last month.

Such responsiveness is the key to Radware's success.

RELATED PROCEEDINGS APPENDIX

(empty)